Flavor Symmetry and
Galois Group of Elliptic Curves

Chuichiro HATTORI, [a] [*] Mamoru MATSUNAGA,[b] [†]

Takeo MATSUOKA,[b,c] [‡] and Kenichi NAKANISHI,[d] [§]

[a]*Science Division, General Education, Aichi Institute of Technology,*
Toyota 470-0392, JAPAN
[b]*Department of Physics Engineering, Mie University,*
Tsu 514-8507, JAPAN
[c]*Chubu University, Kasugai 487-8501, JAPAN*
[d]*Department of Sustainable Resource Science, Mie University,*
Tsu 514-8507, JAPAN

Abstract

A new approach to the generation structure of fermions is proposed. We consider a brane configuration in which the brane intersection yields a two-torus in the extra space. It is assumed that the two-torus is discretized and is given by the torsion points of the elliptic curve over $\mathbb{Q}$. We direct our attention to the arithmetic structure of the elliptic curve with complex multiplication (CM). In our approach the flavor symmetry including the R-parity has its origin in the Galois group of elliptic curves with CM. We study the possible types of the Galois group. The Galois group is shown to be an extension of $\mathbb{Z}_2$ by some abelian group. A phenomenologically viable example of the Galois group is presented, in which the characteristic texture of fermion masses and mixings is reproduced and the mixed-anomaly conditions are satisfied.

[*]E-mail: hattori@aitech.ac.jp

[†]E-mail: matsuna@phen.mie-u.ac.jp

[‡]E-mail: t-matsu@siren.ocn.ne.jp

[§]E-mail: nakanisi@bio.mie-u.ac.jp

1 Introduction

The generation structure of quarks and leptons forms the major outstanding problem of particle physics. In order to solve this problem, it is indispensable for us to introduce basic ingredients other than gauge symmetry. The characteristic texture of fermion masses and mixings strongly suggests the existence of some kinds of underlying discrete symmetry. Furthermore, in the minimal supersymmetric standard model (MSSM) the additional discrete symmetry, that is, the R-parity ought to be introduced to forbid unfavorable interactions which bring about the fast proton decay. It is natural that the R-parity is combined with the usual flavor symmetry and that the flavor symmetry is interpreted in a broader sense including the R-parity. Up to now, many attempts have been made on the usual flavor symmetry. For instance, various types of discrete subgroup of $SU(2)$ and $SU(3)$ have been taken as candidates of the usual flavor symmetry in many articles [1]. In these attempts, however, various types of the usual flavor symmetry are assumed to be temporarily applicable and individual analyses have been made as to whether the observed texture is derived from the assumed flavor symmetry. At present, no one has a first-principle guide to single one symmetry out of many candidates. In this paper we propose an approach to the flavor symmetry including the R-parity different from existing ones. We take the view that the flavor symmetry stems from the structure of the extra space. It is known that the geometry of the Calabi-Yau manifold is closely linked to the arithmetic structure of some algebraic number field of finite degree as well as to the 2-dimensional rational conformal field theory (RCFT) [2, 3]. In view of this fact it is natural that the flavor symmetry can be traced back to the arithmetic structure associated with the extra space. In this paper we direct our attention to elliptic curves as the extra space and propose that the flavor symmetry has its origin in the Galois group of elliptic curves with complex multiplication (CM). Our approach results in the flavor symmetry being restricted to the extension of $\mathbb{Z}_2$ by some abelian group.

We postulate that there exist two kinds of brane and that the intersection of these kinds of brane gives $M_4 \times T^2$, where M_4 represents 4-dimensional spacetime. The two-torus T^2 in the extra dimensional space is given by the elliptic curve E. We study the structure of the extra space on the following assumptions.

- The elliptic curve E is defined over $\mathbb{Q}$.

  - This is linked to a quantization for the shape of E.

2

- The elliptic curve E has CM.

  - This is suggested from the arithmetic structure of RCFT.

- The two-torus is discretized. The discrete two-torus is all of the m-torsion points $E[m]$ of the elliptic curve E over $\mathbb{Q}$ ($m \in \mathbb{Z}_+$).

  - This implies that the size of the two-torus is quantized and is m in fundamental unit.

The elliptic curve E conceals a peculiar discrete symmetry, i.e., the Galois group of E.

In the brane picture the quark/lepton superfields and the Higgs superfields are equally described in terms of open strings with both ends attached to $E[m]$. Although the endpoints of an open string are restricted to lie on the $E[m]$, they are free in the direction along the $E[m]$. We speculate that, according as an orientable open string, we have some kind of mapping from $E[m]$ to $E[m]$. Thus we take the following hypothesis.

- An open string corresponds to a one-to-one mapping from $E[m]$ to $E[m]$.

The one-to-one mapping from $E[m]$ to $E[m]$ induces an action on the Galois extension field generated by the coordinates of all of $E[m]$ and this map specifies an element of the automorphism group of the Galois extension field.

We now illustrate the above-mentioned assumptions and hypothesis in order. Let us consider the lattice Λ with periods ω_1 and ω_2 as

$$\Lambda = \{\omega = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2 \mid \omega_1,\ \omega_2 \in \mathbb{C},\ \mathrm{Im}(\omega_1/\omega_2) > 0\}. \tag{1}$$

The lattice Λ defines an elliptic curve E_Λ through the one-to-one complex analytic map

$$\begin{aligned}
\mathbb{C}/\Lambda\ &\longrightarrow\ E_\Lambda\ :\ y^2 = 4\,x^3 - g_2(\Lambda)\,x - g_3(\Lambda), \\
u\ &\longmapsto\ (x,\ y) = (\wp(u;\ \Lambda),\ \wp'(u;\ \Lambda)),
\end{aligned} \tag{2}$$

where $\wp(u;\ \Lambda)$ is the Weierstrass $\wp$-function relative to the lattice Λ. The set of points of $\mathbb{C}/\Lambda$ forms an additive group. The map $\mathbb{C}/\Lambda \to E_\Lambda$ preserves its additive group structure and gives the isomorphism $\mathrm{End}(\mathbb{C}/\Lambda) \cong \mathrm{End}(E_\Lambda)$. Elliptic curves E_Λ are

classified via the $\mathbb{C}$-isomorphism related to the homothety of the lattice Λ and a $\mathbb{C}$-isomorphism class is denoted by $\{E_\Lambda\}$. As a representative of $\{E_\Lambda\}$ we can choose the elliptic curve determined by the normalized lattice $\Lambda_\tau = \{\mathbb{Z} + \mathbb{Z}\tau\}$, where $\tau = \omega_1/\omega_2$ is the complex structure parameter of the elliptic curve. If the elliptic curve E_Λ has CM, then the complex structure parameter τ is a root of some quadratic equation with integer coefficients and the algebraic extension of $\mathbb{Q}$ associated with E_Λ, $K = \mathbb{Q}(\tau)$, becomes a quadratic imaginary field.

The j-invariant $j(E_\Lambda)$, which is the standard modulus of the elliptic curve E_Λ, is a function depending only on τ. When the elliptic curve E_Λ possesses CM, $j(E_\Lambda)$ becomes an algebraic integer and degree of extension of the field $\mathbb{Q}(j(E_\Lambda))/\mathbb{Q}$ is equal to the class number of the quadratic imaginary field $K = \mathbb{Q}(\tau)$ [4]. Furthermore, $\mathbb{Q}(j(E_\Lambda))$ is the minimal field of definition for the $\mathbb{C}$-isomorphism class $\{E_\Lambda\}$. As mentioned above, we take the elliptic curve E_Λ over $\mathbb{Q}$. Then we have

$$j(E_\Lambda) \in \mathbb{Q} \tag{3}$$

for the standard modulus. This means that K has the class number 1. This implies a *quantization* for the shape of E_Λ.

As shown in the Gepner model [2], the geometry of Calabi-Yau manifold is closely linked to RCFT. In addition, RCFT is also related to algebraic number field of finite degree. In fact, the fusion rule in RCFT [5] yields some commutative ring which is isomorphic to ring of integers of algebraic number field determined by the fusion rule [3]. This suggests that the geometry of Calabi-Yau manifold could be studied in terms of arithmetic structure of the algebraic number field. Furthermore, RCFT also connects with elliptic curves through their modular properties. It is shown that in addition to the multiplication-by-n ($n \in \mathbb{Z}_+$) endomorphisms, the elliptic curve corresponding to the $c = 2$ RCFT possesses extra endomorphism called CM [6].

When the two-torus in the extra space is small in size, it is plausible that the two-torus is considered to be discretized. Concretely, the discrete extra space is taken as all of the m-torsion points

$$E_\Lambda[m] = \{\ P \in E_\Lambda \mid m\,P = \mathcal{O}\} \tag{4}$$

of the elliptic curves E_Λ with CM, where $\mathcal{O}$ is the zero element of additive group on E_Λ. We consider the case $m = p^e$ with a prime number p and $e \in \mathbb{Z}_+$. $E_\Lambda[m]$ on

which the both endpoints of an open string lie has the structure

$$E_\Lambda[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}. \tag{5}$$

A point on $E_\Lambda[m]$ is expressed as $P_l = (x_l,\ y_l) = (\wp(u_l;\ \Lambda),\ \wp'(u_l;\ \Lambda))$ with $l = (l_1,\ l_2)$ and $u_l = (l_1\omega_1 + l_2\omega_2)/m$ where $l_1,\ l_2 = 0, \cdots m - 1$.

Let us consider an orientable open string which corresponds to a matter superfield Φ_ν. Here the matter superfield Φ_ν represents the quark/lepton superfield and the Higgs superfield classified by the generation. The subscript ν represents the degree of freedom of the flavor charge. Since the string is free in the direction along the $E_\Lambda[m]$, the endpoint P_l runs over all points of $E_\Lambda[m]$. Each point P_l of $E_\Lambda[m]$ is accompanied by another endpoint $P_{l'}$ of $E_\Lambda[m]$. The matter superfield Φ_ν is characterized by a set of the ordered pairs of their endpoints $(P_l,\ P_{l'})$ denoted by $\{(P_l,\ P_{l'})\}_\nu$. Our hypothesis means that in each set $\{(P_l,\ P_{l'})\}_\nu$ we can introduce the mapping

$$\phi_\nu\ :\ P_l \longmapsto P_{l'} \qquad \text{for all } P_l \in E_\Lambda[m] \tag{6}$$

which is a one-to-one map from $E_\Lambda[m]$ to $E_\Lambda[m]$.

Elliptic curves E_Λ have the multiplication-by-n ($n \in \mathbb{Z}_+$) endomorphism, which induces the endomorphism of $E_\Lambda[m]$. In particular, when $(n,\ m) = 1$, this endomorphism of $E_\Lambda[m]$ is an automorphism. The matter superfield Φ_ν is invariant under the multiplication-by-n automorphism. On the other hand, the transformation of $P_l = (x_l,\ y_l)$ into $P_{l'} = (x_{l'},\ y_{l'})$ induces the action on the Galois extension field $L = K(E_\Lambda[m])$ which is the extension of field $K(j(E_\Lambda))$ generated by the coordinates of all of $E_\Lambda[m]$. We notice that $K(j(E_\Lambda)) = K$ because of Eq. (3). The one-to-one mapping ϕ_ν corresponds to a conjugation mapping of L. Namely, for each Φ_ν the mapping ϕ_ν is identified as an element of the automorphism group of L, i.e., the Galois group. The set Φ_ν forms a regular representation of the Galois group. In our point of view the Galois group of $E_\Lambda[m]$ is precisely the flavor symmetry.

The quadratic imaginary field $K/\mathbb{Q}$ leads to the Galois group $Gal(K/\mathbb{Q}) = \mathbb{Z}_2$. The field $L = K(E_\Lambda[m])$ is a Galois extension of K and the Galois group

$$H = Gal(L/K) = \mathrm{Aut}_K L \tag{7}$$

is abelian [4]. In addition, L is a Galois extension of $\mathbb{Q}$ and the Galois group

$$G = Gal(L/\mathbb{Q}) = \mathrm{Aut}_\mathbb{Q} L \tag{8}$$

is derived. Each element of the Galois group G acts on $E_\Lambda[m]$. We thus obtain the Galois representation

$$\rho_m : Gal(L/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z}), \tag{9}$$

which is a one-to-one homomorphism. G is an extension of $\mathbb{Z}_2$ by the abelian kernel H. Among such types of the group we proceed to explore phenomenologically viable candidates of the flavor symmetry. In general, L is not always an abelian extension of $\mathbb{Q}$. In many cases G contains the dihedral group D_n $(n \geq 3)$ but not the symmetric group S_n $(n \geq 4)$.

This paper is organized as follows. A brief explanation of the elliptic curves with CM is given in section 2. In section 3 we study the main features of the Galois group G derived from the m-torsion points $E_\Lambda[m]$ $(m \in \mathbb{Z}_+)$ of the elliptic curves E_Λ with CM. We postulate that there exist two kinds of brane and that the intersection of these kinds of brane gives $M_4 \times T^2$, where the T^2 is given by E_Λ. In addition, we take E_Λ over $\mathbb{Q}$. This corresponds to the quantization condition on the shape of E_Λ. We propose a new interpretation that the flavor symmetry including the R-parity has its origin in the Galois group G which stems from the arithmetic structure of elliptic curves with CM. Concrete examples of the Galois group G are also shown for the cases $\tau = i$, ω, where $\omega = \exp(2\pi i/3)$. In section 4 we discuss the group extension G of $\mathbb{Z}_2$ by an abelian kernel H and classify possible Galois groups G in which $\mathbb{Z}_2$ is homomorphically embedded in G. In section 5 we apply the Galois group $G = \{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_N$ to $SU(6) \times SU(2)_R$ string-inspired model as an example of the flavor symmetry. $\mathbb{Z}_2 = Gal(K/\mathbb{Q})$ is identified with the R-parity. We take the brane configuration in which one of two kinds of the brane has the degree of freedom of $SU(6)$ gauge group and the other has that of $SU(2)_R$ gauge group. This example exhibits a phenomenologically viable solution with $N = 31$ in which the characteristic texture of fermion masses and mixings is reproduced. Furthermore, it is also shown that this solution satisfies the mixed-anomaly conditions. Section 6 is devoted to summary and discussion. In Appendix we consider the group extension of $\mathbb{Z}_2$ by an abelian group H.

2 Elliptic curves with CM

In this section we give a brief explanation of the elliptic curve E and CM on E. After that, we will discuss the effective theory in which the quark/lepton superfields and the Higgs superfields live in $M_4 \times T^2$, where the T^2 is given by E with CM.

The elliptic curve E_Λ relative to the lattice Λ with periods ω_1 and ω_2 is defined via the one-to-one complex analytic map

$$
\begin{aligned}
\mathbb{C}/\Lambda &\longrightarrow E_\Lambda \;:\; y^2 = 4\,x^3 - g_2(\Lambda)\,x - g_3(\Lambda), \\
u &\longmapsto (x,\,y) = (\wp(u;\,\Lambda),\,\wp'(u;\,\Lambda)).
\end{aligned}
\tag{10}
$$

The functions g_2 and g_3 are expressed in terms of Eisenstein series $G_{2k}(\Lambda)$ as

$$
g_2(\Lambda) = 60\,G_4(\Lambda), \qquad g_3(\Lambda) = 140\,G_6(\Lambda),
$$

where

$$
G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2k}}.
$$

Substituting $2y$ for y and using the notation $g_2(\Lambda) = -4A$ and $g_3(\Lambda) = -4B$, we obtain the standard form of the elliptic curve

$$
E_\Lambda \;:\; y^2 = f(x) = x^3 + Ax + B.
\tag{11}
$$

The modular discriminant of the elliptic curve E_Λ is given by

$$
\Delta(\Lambda) = g_2(\Lambda)^3 - 27\,g_3(\Lambda)^2 = -16\left(4\,A^3 + 27\,B^2\right).
$$

The set of points of an elliptic curve forms an additive group and the group law is given by rational functions. The map $\mathbb{C}/\Lambda \to E_\Lambda$ defined by Eq. (10) preserves its additive group structure and gives the isomorphism $\mathrm{End}(\mathbb{C}/\Lambda) \cong \mathrm{End}(E_\Lambda)$. When we carry out the homothety of Λ

$$
\Lambda \longrightarrow \lambda\Lambda, \qquad \lambda \in \mathbb{C}^*,
\tag{12}
$$

the coefficients A and B are transformed as

$$
A \longrightarrow \lambda^{-4}A, \qquad B \longrightarrow \lambda^{-6}B.
$$

If we substitute $(\lambda^{-2}x, \ \lambda^{-3}y)$ for $(x, \ y)$, Eq. (11) remains unchanged. For this reason, elliptic curves E_Λ are classified via the $\mathbb{C}$-isomorphism. As a representative of a $\mathbb{C}$-isomorphism class $\{E_\Lambda\}$ we can choose E_{Λ_τ} relative to the normalized lattice $\Lambda_\tau = \{\mathbb{Z} + \mathbb{Z}\tau\}$ with $\tau = \omega_1/\omega_2$. Here, the complex structure parameter τ of two-torus T^2 is defined in the upper half-plane $U = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$. However, many τ's give the same lattice Λ_τ. This is because there remains the degree of freedom of modular transformations. Hence, we introduce the quotient space $\Gamma(1)\backslash U^*$ given by the fundamental region

$$\mathcal{F} = \{\tau \in U \mid |\tau| \geq 1, \ |\operatorname{Re}\tau| \leq \frac{1}{2}\}, \tag{13}$$

where $\Gamma(1)$ is the modular group and $U^* = U \cup \mathbb{P}^1(\mathbb{Q})$. If we take the value of τ in $\mathcal{F}$, τ has the one-to-one correspondences to the lattice Λ_τ. The functions $g_2(\tau) := g_2(\Lambda_\tau)$ and $g_3(\tau) := g_3(\Lambda_\tau)$ are the modular forms of weight 4 and 6 for $\Gamma(1)$, respectively. The modular discriminant $\Delta(\tau)$ is the cusp form of weight 12 and expressed as

$$\Delta(\tau) = g_2(\tau)^3 - 27\,g_3(\tau)^2 = (2\pi)^{12}\eta(\tau)^{24},$$

where $\eta(\tau)$ stands for the Dedekind η-function.

Next we proceed to explain CM on the elliptic curve. In general, using the isomorphism $\operatorname{End}(E_\Lambda) \cong \operatorname{End}(\mathbb{C}/\Lambda)$, we can study the automorphism on $\mathbb{C}/\Lambda$ instead of that on E_Λ. The elliptic curve corresponding to RCFT possesses not only the multiplication-by-n ($n \in \mathbb{Z}_+$) endomorphism but also CM. Namely, there exists a complex number μ ($\notin \mathbb{R}$) such that $\mu\Lambda \subset \Lambda$. In the elliptic curve E_Λ with CM, τ is a root of some quadratic equation with integer coefficients. The discriminant of the quadratic equation D should be negative. Thus we can define the quadratic imaginary field $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\tau)$, which is the algebraic extension of $\mathbb{Q}$ associated with E_Λ. This means that E_Λ possesses CM by K.

The j-invariant $j(E_\Lambda)$ depends only upon τ and so is denoted by $j(\tau)$. The explicit form is

$$j(\tau) = \frac{(12\,g_2(\tau))^3}{\Delta(\tau)} = 1728\,\frac{4A^3}{4A^3 + 27B^2},$$

which is a modular function of weight 0. For the elliptic curve with CM, $j(E_\Lambda)$ becomes an algebraic integer and $\mathbb{Q}(j(E_\Lambda))$ is the minimal field of definition for the

$\mathbb{C}$-isomorphism class $\{E_\Lambda\}$. The class $\{E_\Lambda\}$ is isomorphic to the ideal class group of R_K which is the ring of integers of K. The degree of extension of the field $\mathbb{Q}(j(E_\Lambda))/\mathbb{Q}$ is equal to the class number h_K of the quadratic imaginary field $K = \mathbb{Q}(\tau)$ [4].

Here, we consider E_Λ over $\mathbb{Q}$. This leads to

$$j(E_\Lambda) \in \mathbb{Q} \tag{14}$$

and $h_K = 1$. This strongly constrains the value of τ and then implies the quantization for the shape of E_Λ. Incidentally, it is known that there are only nine quadratic imaginary fields $\mathbb{Q}(\sqrt{D})$ of $h_K = 1$ [4]. These fields are the cases of

$$-D = 1, \ 2, \ 3, \ 7, \ 11, \ 19, \ 43, \ 67, \ 163. \tag{15}$$

In the next section, we take up the cases $-D = 1, \ 3$ as simple examples of the Galois group of the elliptic curves with CM.

3 Galois groups on elliptic curves

In our approach based on the brane picture, the quark/lepton superfields and the Higgs superfields are described in terms of open strings with both ends attached to the extra space E_Λ. These endpoints of open strings are free in the direction along the E_Λ. In this paper the extra space is taken to be all of the m-torsion points $E_\Lambda[m]$ of the elliptic curves E_Λ with CM. Thus the endpoints of open strings lie on $E_\Lambda[m]$. A point on $E_\Lambda[m]$ is expressed as $P_l = (x_l, \ y_l)$ with $l = (l_1, \ l_2)$. Since the string is free in the direction along the $E_\Lambda[m]$, the endpoint P_l runs over all points of $E_\Lambda[m]$. Each point P_l of $E_\Lambda[m]$ is accompanied by another endpoint $P_{l'}$ of $E_\Lambda[m]$. The matter superfield Φ_ν is characterized by a set of the ordered pairs of their endpoints $(P_l, \ P_{l'})$ denoted by $\{(P_l, \ P_{l'})\}_\nu$. Our hypothesis insists that in each set $\{(P_l, \ P_{l'})\}_\nu$ we can introduce the mapping

$$\phi_\nu \ : \ P_l \ \longmapsto \ P_{l'} \qquad \text{for all } P_l \in E_\Lambda[m] \tag{16}$$

which is a one-to-one map from $E_\Lambda[m]$ to $E_\Lambda[m]$. In order to clarify the meaning of the mapping ϕ_ν it is proper to take p-adic metric [7]. When both $(P_l, \ P_{l'})$ and $(P_k, \ P_{k'})$ are contained in the set $\{(P_l, \ P_{l'})\}_\nu$, we put the condition

$$|P_l - P_k|_p = |P_{l'} - P_{k'}|_p \tag{17}$$

for the p-adic distances of the both endpoints, where $|P_l|_p \equiv \text{Max}\{|l_1/m|_p,\ |l_2/m|_p\}$ and $|P_0|_p = |\mathcal{O}|_p = 0$. This condition bears some analogy with the parallel transport in the sense of the ordinary distance. From the additive group structure on $E_\Lambda[m]$, we have $P_l - P_k = P_{l-k}$. Then the above condition is rewritten as $|P_{l-k}|_p = |P_{l'-k'}|_p$. If we take $l' = k' \pmod m$, we have $|P_{l-k}|_p = |P_0|_p = |\mathcal{O}|_p = 0$. This leads to $l = k$ $\pmod m$. Consequently, in conjunction with this set $\{(P_l,\ P_{l'})\}_\nu$ we can consider the mapping ϕ_ν. The mapping ϕ_ν is settled for each Φ_ν and exhibits the freedom of the flavor symmetry.

Elliptic curves E_Λ have the multiplication-by-n ($n \in \mathbb{Z}_+$) endomorphisms. In particular, when $(n,\ m) = 1$, $E_\Lambda[m]$ has the multiplication-by-n automorphism. In view of the one-to-one correspondence between Φ_ν and the set $\{(P_l,\ P_{l'})\}_\nu$, the matter superfield Φ_ν is invariant under the multiplication-by-n automorphism and we have

$$\{(P_{nl},\ P_{nl'})\}_\nu \subset \{(P_l,\ P_{l'})\}_\nu \qquad \text{for } n \in \mathbb{Z}_+. \tag{18}$$

In the case $n = m$, $(P_{nl},\ P_{nl'})$ amounts to $(\mathcal{O},\ \mathcal{O})$. If we take $P_k = P_{k'} = \mathcal{O}$ in Eq. (17), we obtain $|P_l|_p = |P_{l'}|_p$. This means that the order of $P_{l'}$ in the additive group coincides with that of P_l. It turns out that the mapping ϕ_ν keeps the order of each point of $E_\Lambda[m]$. Then ϕ_ν is a one-to-one map from $E_\Lambda[m]$ to $E_\Lambda[m]$.

On the other hand, $E_\Lambda[m]$ equips the Galois extension field L. In fact, L is the extension of field $K(j(E_\Lambda))$ generated by the coordinates of all of $E_\Lambda[m]$. The transformation of $P_l = (x_l,\ y_l)$ into $P_{l'} = (x_{l'},\ y_{l'})$ acts on the Galois extension field L. Since ϕ_ν is one-to-one and order-preserving, ϕ_ν corresponds to a conjugation mapping of L. This means that the mapping ϕ_ν is an element of the automorphism group of L. Because of Eq. (3) we have $K(j(E_\Lambda)) = K$. The Galois extension field $L = K(E_\Lambda[m])$ has many important features. Concretely, the Galois group

$$H = Gal(L/K) = \text{Aut}_K L \tag{19}$$

is abelian. Furthermore, L is also the Galois extension of $\mathbb{Q}$ and its Galois group

$$G = Gal(L/\mathbb{Q}) = \text{Aut}_\mathbb{Q} L \tag{20}$$

is the group extension of $\mathbb{Z}_2 = Gal(K/\mathbb{Q})$ by an abelian kernel H, as noted in section 4. In general, L is not an abelian extension of $\mathbb{Q}$. Each element of the Galois group G acts on $E_\Lambda[m]$. We obtain the Galois representation

$$\rho_m : Gal(L/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z}). \tag{21}$$

10

Thus the map ϕ_ν represents an element of G. The set Φ_ν forms a regular representation of G. The Galois group G is precisely the flavor symmetry.

Here we touch upon a physical interpretation of $E_\Lambda[m]$. We may consider that the extra space $E_\Lambda[m]$ is quantized in unit of the size given by the fundamental period-parallelogram $\Lambda_0 = m^{-1}\Lambda$. Thus m represents the size of the extra space $E_\Lambda[m]$ in unit of E_{Λ_0}. The Kähler modulus ρ of the E_Λ becomes $\rho = m^2\rho_0$, where ρ_0 is the Kähler modulus of E_{Λ_0}. It is natural that the size of E_{Λ_0} corresponds to the fundamental scale of the string theory, which is nearly equal to the Planck scale.

Among the m-torsion points on $\mathbb{C}/\Lambda$, the number of the points of order m is denoted by N_m. The set of the points of order m is given by

$$\{u \mid u \in \mathbb{C}/\Lambda, \ mu \in \Lambda, \ m'u \notin \Lambda \text{ for } m' < m\}.$$

Any elements of H give the mapping from the points of order m to those of order m on $\mathbb{C}/\Lambda$. In the case $m = p^e$ with a prime number p we have

$$N_m = (p^2 - 1)\, p^{2(e-1)}. \tag{22}$$

In the case $m = 2$ we get $N_m = 3$, otherwise $N_m = $ even. The x-coordinates of the points of order m among the m-torsion points on E_Λ are the roots of the equation over $\mathbb{Q}$

$$\psi_m(x) = \prod_u (x - \wp(u)) = 0. \tag{23}$$

Since the Weierstrass $\wp$-function is an even function, the above product is taken over 3 points of order 2 on $\mathbb{C}/\Lambda$ for $m = 2$, otherwise over $N_m/2$ points. Therefore, the degree of the polynomial $\psi_m(x)$ is 3 for $m = 2$, otherwise $N_m/2$.

When j-invariant and m are given, the Galois group H of L/K changes with changing the elliptic curve E_Λ. The maximum value of the order $\sharp H$ of H is N_m. In order that the order $\sharp H$ of H takes its maximum value, the polynomial $\psi_m(x)$ is needed to be irreducible over $\mathbb{Q}$. In general, if the polynomial $\psi_m(x)$ is irreducible over $\mathbb{Q}$, we have the relation $(\sharp H)|N_m$. On the other hand, if the polynomial $\psi_m(x)$ is reducible over $\mathbb{Q}$, $\sharp H$ is smaller than N_m and is not always a divisor of N_m.

As concrete examples of the elliptic curves with CM we now consider two cases $-D = 1, 3$ which mean $\tau = i, \omega$, where $\omega = \exp(2\pi i/3)$. For these cases we illustrate the Galois group G coming from $E_\Lambda[m]$. Since $g_3(i) = 0$ and $g_2(\omega) = 0$, the value of $j(E_\Lambda)$ is 1728 and 0, respectively, that is, $j \in \mathbb{Q}$. Then E_Λ associated with $\tau = i, \omega$

Table 1: $m = 3$ torsion points on elliptic curve E_Λ : $y^2 = x^3 + 1$

	$q = 0$	1	2
$p = 0$	$\mathcal{O}$	$(-\sqrt[3]{4},\ \sqrt{3}\,i)$	$(-\sqrt[3]{4},\ -\sqrt{3}\,i)$
1	$(0,\ 1)$	$(-\sqrt[3]{4}\,\omega,\ \sqrt{3}\,i)$	$(-\sqrt[3]{4}\,\omega^2,\ -\sqrt{3}\,i)$
2	$(0,\ -1)$	$(-\sqrt[3]{4}\,\omega^2,\ \sqrt{3}\,i)$	$(-\sqrt[3]{4}\,\omega,\ -\sqrt{3}\,i)$

is $\mathbb{C}$-isomorphic to the elliptic curve $y^2 = x^3 + x$ and $y^2 = x^3 + 1$, respectively. Here we focus on the elliptic curves over $\mathbb{Q}$

$$E_\Lambda \quad : \quad y^2 = x^3 + A\,x, \qquad A \in \mathbb{Z}, \tag{24}$$

$$E_\Lambda \quad : \quad y^2 = x^3 + B, \qquad B \in \mathbb{Z}, \tag{25}$$

which is $\mathbb{C}$-isomorphic to the elliptic curve $y^2 = x^3 + x$ and $y^2 = x^3 + 1$, respectively.

For illustration we first take up the 3-torsion points on the elliptic curve E_Λ : $y^2 = x^3 + 1$ and study the Galois group $Gal(K(E_\Lambda[3])/\mathbb{Q})$. All of the 3-torsion points are described in terms of two bases P and Q as

$$E_\Lambda[3] = \{p\,P + q\,Q \mid p,\ q \in \mathbb{Z}/3\mathbb{Z}\}. \tag{26}$$

Consequently, the torsion points are exhibited by 2-dimensional representation of the Galois group. In the present case the coordinates $(x,\ y)$ of the bases P and Q are given by

$$P = (0,\ 1), \quad Q = (-\sqrt[3]{4},\ \sqrt{3}i).$$

All of the 3-torsion points are shown in Table 1. The Galois extension field becomes $L = K(E_\Lambda[3]) = \mathbb{Q}(\omega,\ \sqrt[3]{4})$ and the Galois group of L/K is $H = \mathbb{Z}_3$. Although $N_m = 8$ for the case $m = 3$, the polynomial $\psi_3(x)$ for E_Λ : $y^2 = x^3 + 1$ is reducible over $\mathbb{Q}$. This results in $\sharp H = 3$ and then $(\sharp H) \nmid N_m$. The generators b and a of the Galois group G are defined by

$$b \quad : \quad \omega \to \omega^2,$$

$$a \quad : \quad \sqrt[3]{4} \to \sqrt[3]{4}\omega.$$

Table 2: $m = 3$ torsion points on elliptic curve E_Λ : $y^2 = x^3 + x$

	$q = 0$	1	2
$p = 0$	$\mathcal{O}$	$(-\alpha_-,\ i\beta_{1-})$	$(-\alpha_-,\ -i\beta_{1-})$
1	$(\alpha_-,\ \beta_{1-})$	$(-i\alpha_+,\ \frac{(1+i)}{\sqrt{2}}\beta_{1+})$	$(i\alpha_+,\ \frac{(1-i)}{\sqrt{2}}\beta_{1+})$
2	$(\alpha_-,\ -\beta_{1-})$	$(i\alpha_+,\ \frac{(-1+i)}{\sqrt{2}}\beta_{1+})$	$(-i\alpha_+,\ \frac{(-1-i)}{\sqrt{2}}\beta_{1+})$

Taking the Galois representation $\rho_3 : Gal(K(E_\Lambda[3])/\mathbb{Q}) \to GL_2(\mathbb{Z}/3\mathbb{Z})$, we have

$$\rho_3(b) \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho_3(a) \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (\text{mod } 3).$$

In this case we obtain the relations

$$b^2 = a^3 = e, \quad b\,a\,b = a^{-1} \tag{27}$$

and the Galois group becomes the dihedral group

$$G = Gal(\mathbb{Q}(E_\Lambda[3])/\mathbb{Q}) = \mathbb{Z}_2 \ltimes \mathbb{Z}_3 = D_3. \tag{28}$$

As the second example we take up the 3-torsion points on the elliptic curve E_Λ : $y^2 = x^3 + x$ and study the Galois group $Gal(K(E_\Lambda[3])/\mathbb{Q})$. In the present case the coordinates $(x,\ y)$ of the bases P and Q are given by

$$P = (\alpha_-,\ \beta_{1-}), \quad Q = (-\alpha_-,\ i\beta_{1-}).$$

In Table 2 all of the 3-torsion points are found, where

$$\alpha_\pm = \frac{\sqrt{3} \pm 1}{\sqrt{2\sqrt{3}}}, \quad \beta_{1\pm} = \sqrt{\sqrt{3} \pm 1}\,\left(2/\sqrt{27}\right)^{\frac{1}{4}}.$$

13

$\alpha_\pm$ and $\beta_{1+}/\sqrt{2}$ are described in terms of β_{1-} as

$$\alpha_+ \;=\; \frac{2}{3\,\beta_{1-}^2},$$

$$\alpha_- \;=\; \frac{2}{3\,\beta_{1+}^2} \;=\; \frac{3}{16}\,\beta_{1-}^2\,(3\,\beta_{1-}^4 + 4),$$

$$\frac{1}{\sqrt{2}}\,\beta_{1+} \;=\; \frac{8\,\beta_{1-}}{9\,\beta_{1-}^4 + 4}.$$

Thus, the Galois extension field is $L = K(E_\Lambda[3]) = \mathbb{Q}(i,\ \beta_{1-})$ and the Galois group of L/K becomes $H = \mathbb{Z}_8$. In this case the polynomial $\psi_3(x)$ is irreducible over $\mathbb{Q}$. The generators b and a of the Galois group G are defined by

$$b \quad : \quad i \longrightarrow -i,$$

$$a \quad : \quad \beta_{1-} \longrightarrow \frac{(-1+i)}{\sqrt{2}}\,\beta_{1+}.$$

Taking the Galois representation $\rho_3 : Gal(K(E_\Lambda[3])/\mathbb{Q}) \to GL_2(\mathbb{Z}/3\mathbb{Z})$, we have

$$\rho_3(b) \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \rho_3(a) \equiv \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix} \qquad (\mathrm{mod}\ 3).$$

These generators hold the relations

$$b^2 = a^8 = e, \qquad b\,a\,b = a^3. \tag{29}$$

The Galois group G is of the form

$$G = Gal(\mathbb{Q}(E_\Lambda[3])/\mathbb{Q}) = \mathbb{Z}_2 \ltimes \mathbb{Z}_8. \tag{30}$$

Although this group differs from D_8, the relation

$$b\,a^2\,b = a^{-2} \tag{31}$$

is satisfied and then we obtain $\langle b,\ a^2 \rangle = D_4 \subset G = \mathbb{Z}_2 \ltimes \mathbb{Z}_8$.

14

Table 3: Galois Groups on E_Λ : $y^2 = x^3 + A\,x$

E_Λ	$y^2 = x^3 + x$	$y^2 = x^3 + 2x$
$L = K(E_\Lambda[2])$	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{2}\,i)$
$G = Gal(L/\mathbb{Q})$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
$L = K(E_\Lambda[3])$	$\mathbb{Q}(i,\ \beta_{1-})$	$\mathbb{Q}(i,\ \beta_{2-})$
$G = Gal(L/\mathbb{Q})$	$\mathbb{Z}_2 \ltimes \mathbb{Z}_8$	$\mathbb{Z}_2 \ltimes \mathbb{Z}_8$
$L = K(E_\Lambda[4])$	$\mathbb{Q}(i,\ \sqrt{2})$	$\mathbb{Q}(i,\ \sqrt[4]{2})$
$G = Gal(L/\mathbb{Q})$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4

Table 4: Galois Groups on E_Λ : $y^2 = x^3 + B$

E_Λ	$y^2 = x^3 + 1$	$y^2 = x^3 + 2$
$L = K(E_\Lambda[2])$	$\mathbb{Q}(\omega)$	$\mathbb{Q}(\omega,\ \sqrt[3]{2})$
$G = Gal(L/\mathbb{Q})$	$\mathbb{Z}_2$	D_3
$L = K(E_\Lambda[3])$	$\mathbb{Q}(\omega,\ \sqrt[3]{4})$	$\mathbb{Q}(\omega,\ \sqrt{2})$
$G = Gal(L/\mathbb{Q})$	D_3	$\mathbb{Z}_2 \times \mathbb{Z}_2$
$L = K(E_\Lambda[4])$	$\mathbb{Q}(\omega,\ \sqrt[4]{27}/\sqrt{2})$	$\mathbb{Q}(\omega,\ \sqrt[3]{2},\ \sqrt[4]{27})$
$G = Gal(L/\mathbb{Q})$	D_4	$\mathbb{Z}_2 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3)$

In Tables 3 and 4 we summarize the Galois extension fields $L = K(E_\Lambda[m])$ and the Galois group $G = Gal(L/\mathbb{Q})$ for the cases $m = 2,\ 3,\ 4$, where the elliptic curves E_Λ are taken as $y^2 = x^3 + Ax$ and $y^2 = x^3 + B$ with $A,\ B = 1,\ 2$, respectively. In Table 3 we use the notation $\beta_{2-} = \beta_{1-}/2^{1/4}$. In particular, it is worth noting that in the 4-torsion points on E_Λ : $y^2 = x^3 + 2$ the polynomial $\psi_4(x)$ is irreducible over $\mathbb{Q}$ and $\sharp H$ takes the maximum value $\sharp H = N_m = 12$. In this case we obtain the Galois group $G = \mathbb{Z}_2 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3)$. Their corresponding generators b, a_1, a_2 and a_3 hold the relations

$$b\,a_1\,b = a_2, \qquad b\,a_3\,b = a_3^{-1} \tag{32}$$

and a_1, a_2 and a_3 are commutable with each other.

The Galois group G is, as described in the next section, the extension of $\mathbb{Z}_2$ by an abelian group H, $G/H \cong \mathbb{Z}_2$. There are many types of the Galois group G. As seen in explicit examples, there exist both the abelian and the nonabelian G. In many nonabelian cases, G contains the dihedral group D_n ($n \geq 3$) but not the symmetric group S_n ($n \geq 4$). In the next section and Appendix we discuss the detailed classification of the Galois group G given by the extension of $\mathbb{Z}_2$ by an abelian group H.

4 Extension of $\mathbb{Z}_2$ by an abelian kernel H

In the foregoing sections we have proposed a hypothesis that the Galois group $G = Gal(L/\mathbb{Q})$ of the Galois extension field $L = K(E[m])$, generated by adjoining the torsion points $E[m]$ of the elliptic curve E_Λ to the quadratic imaginary field $K = \mathbb{Q}(\tau)$, should be regarded as the flavor symmetry. We have calculated the group G explicitly in the cases of $m = 3, 4$. It is, however, difficult to implement the same calculation for larger values of m. In this section we investigate general properties of the Galois group G of the extension $L/\mathbb{Q}$. We will see that the Galois group $G = Gal(L/\mathbb{Q})$ is an extension of $\mathbb{Z}_2$ by some abelian group H and that this extension is a semidirect product group $\mathbb{Z}_2 \ltimes H$.

4.1 Fundamental theorem of Galois theory

The Galois group $G = Gal(L/\mathbb{Q})$ has an important property described by the fundamental theorem of Galois theory [8]. This theorem states that, in a Galois extension L/F, any intermediate extension K/F is also a Galois extension if and only if the group $Gal(L/K)$ is a normal subgroup of $Gal(L/F)$. The theorem also asserts that the three groups are related to each other as $Gal(L/F)/Gal(L/K) \cong Gal(K/F)$. Applying the theorem to the three number fields $L = K(E[m])$, $K = \mathbb{Q}(\tau)$ and $F = \mathbb{Q}$, we obtain the isomorphism $G/H \cong Gal(K/\mathbb{Q}) = \mathbb{Z}_2$. As stated in section 3, the group $H = Gal(L/K)$ is abelian. Thus, $G = Gal(L/\mathbb{Q})$ is an extension of $\mathbb{Z}_2$ by the abelian kernel $H = Gal(L/\mathbb{Q}(\tau))$.

We further notice that the field $L = K(E[m])$ contains the field $K = \mathbb{Q}(\tau)$ and that the group $Gal(K/\mathbb{Q})$ is generated by complex conjugation map. This map forms a $\mathbb{Q}$-automorphism of L because L is obtained by adjoining the roots of an algebraic

equation with coefficients of rational numbers to K. In such case $\mathbb{Z}_2 \cong Gal(K/\mathbb{Q})$ is a subgroup of $Gal(L/\mathbb{Q})$[¶].

4.2 Semidirect product

In what follows, we focus on the case that $\mathbb{Z}_2$ is homomorphically embedded in G. It is well known in group theory that, in the extension G of a group Q by a group H, $G/H \cong Q$, G is a semidirect product $G = Q \ltimes_\sigma H$ if and only if Q can be homomorphically embedded in G [9]. The subscript σ refers to a homomorphism from Q to the automorphism group of H, $Q \to \text{Aut}\, H$ denoted by $b \mapsto \sigma_b$. The semidirect product $Q \ltimes_\sigma H$ is described in terms of Cartesian product $\{(b,h)\}$ in which the product of two elements (b,h) and (b',h') is defined as

$$(b,h) \cdot (b',h') = (b\,b', \sigma_{b'}(h)\,h') \tag{33}$$

with $\sigma_{b'}(h) = b'\,h\,b'^{-1}$. Identifying $b \in Q$ and $h \in H$ with (b,e), $(e,h) \in Q \times H$ respectively, we obtain

$$b^2 = (b,e) \cdot (b,e) = (b^2, \sigma_b(e)e) = (b^2, e), \tag{34}$$

$$b\,h\,b = (b,e) \cdot (e,h) \cdot (b,e) = (b,h) \cdot (b,e) = (b^2, \sigma_b(h)). \tag{35}$$

In our setting $Q = \mathbb{Z}_2$, the homomorphism σ satisfies $\sigma \cdot \sigma = \text{id}_{\mathbb{Z}_2}$. Because the nontrivial element of $\mathbb{Z}_2$ is only its generator, we shall hereafter denote the generator simply as b. Then Eqs. (34) and (35) become

$$b^2 = e, \quad b\,h\,b = \sigma_b(h). \tag{36}$$

Equation (36) constitutes the fundamental relation of the group $\mathbb{Z}_2 \ltimes_\sigma H$.

4.3 Examples

The fundamental theorem of abelian groups states that a finite abelian group H is, in general, isomorphic to a product of cyclic groups of the form

$$H \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_t},$$

[¶] For a general integral ideal $\mathfrak{a}$ and $L = E_\Lambda[\mathfrak{a}]$, however, $\mathbb{Z}_2$ is not necessarily a subgroup of $G = Gal(L/\mathbb{Q})$ [4].

where $N_i = p_i^{e_i}$ ($p_i \leq p_{i+1}$), $e_i \in \mathbb{Z}_+$ and p_i's are prime numbers. In the remaining part of this section, we explore the semidirect product for the cases of $t = 1, 2$. Since the semidirect product $\mathbb{Z}_2 \ltimes_\sigma H$ is determined by $\sigma_b \in \text{Aut } H$ as dictated in Eq.(36), we examine the possible automorphisms of order two.

4.3.1 $H = \mathbb{Z}_N$ $(N = p^e)$

An automorphism σ_b of H is given by $\sigma_b(a) = a^n$ for a generator a of $\mathbb{Z}_N$. The relation $\sigma_b \cdot \sigma_b = \text{id}_{\mathbb{Z}_2}$ implies $(a^n)^n = a^{n^2} = a$, whose solutions are $n_0 \equiv \pm 1$, $\pm r$ (mod N), where $r = 2^{e-1} + 1$. The latter solution $n_0 \equiv \pm r$ are possible only when $p = 2$ and $e \geq 3$. The semidirect product G becomes

$$G = \left\langle a, b \mid a^N = b^2 = e, \ bab = a^{n_0} \right\rangle.$$

The group G with $n_0 \equiv 1$ is the direct product group and G with $n_0 \equiv -1$ is the dihedral group.

4.3.2 $H = \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ $(N_1 = p_1^{e_1}, \ N_2 = p_2^{e_2}, \ e_1 \leq e_2)$

An automorphism σ_b is given by

$$\begin{cases} \sigma_b(a_1) = a_1^{m_1} a_2^{m_2}, \\ \sigma_b(a_2) = a_1^{n_1} a_2^{n_2}, \end{cases} \tag{37}$$

where a_1 and a_2 are generators of $\mathbb{Z}_{N_1}$ and $\mathbb{Z}_{N_2}$, respectively. In exploring all the possible automorphism of order two, we should pay our attention to the following four points.

- *well-definedness of σ_b*
  We note that m_1, n_1 are defined in mod N_1 and m_2, n_2 in mod N_2, respectively. Automorphic property of σ_b leads to

$$e = \sigma(a_1^{N_1}) = \sigma(a_1)^{N_1} = a_2^{m_2 N_1},$$
$$e = \sigma(a_2^{N_2}) = \sigma(a_2)^{N_2} = a_1^{n_1 N_2},$$

  which requires

$$m_2 N_1 \equiv 0 \pmod{N_2},$$
$$n_1 N_2 \equiv 0 \pmod{N_1}.$$

From these congruence equations, we find that if $p_1 \neq p_2$, then

$$n_1 \equiv 0 \pmod{N_1}, \quad m_2 \equiv 0 \pmod{N_2}, \tag{38}$$

and that, if $p_1 = p_2 =: p$, then

$$p^{e_2 - e_1} | m_2. \tag{39}$$

- *bijectivity of σ_b*
  The case $p_1 \neq p_2$ is essentially reduced to the case given in subsection 4.3.1. The case $p_1 = p_2 =: p$ requires some scrutiny. The homomorphism σ_b given in (37) is bijective only when we have the relations

$$\begin{cases} a_1 = \sigma_b(a_1^{s_1} a_2^{s_2}), \\ a_2 = \sigma_b(a_1^{t_1} a_2^{t_2}) \end{cases}$$

for some $s_1, s_2, t_1, t_2 \in \mathbb{Z}$. These relations are translated into

$$\begin{cases} m_1 s_1 + n_1 s_2 \equiv 1 & \pmod{N_1}, \\ m_2 s_1 + n_2 s_2 \equiv 0 & \pmod{N_2}, \\ m_1 t_1 + n_1 t_2 \equiv 0 & \pmod{N_1}, \\ m_2 t_1 + n_2 t_2 \equiv 1 & \pmod{N_2}. \end{cases} \tag{40}$$

From these equations we can easily find that

$$\sigma_b \text{ is bijective} \iff m_1 n_2 - m_2 n_1 \not\equiv 0 \pmod{p}.$$

- $\sigma_b \cdot \sigma_b = \mathrm{id}_{\mathbb{Z}_2}$
  This leads to

$$\begin{cases} m_1{}^2 + n_1 m_2 \equiv 1 & \pmod{N_1}, \\ m_2(m_1 + n_2) \equiv 0 & \pmod{N_2}, \\ n_1(m_1 + n_2) \equiv 0 & \pmod{N_1}, \\ n_1 m_2 + n_2{}^2 \equiv 1 & \pmod{N_2}. \end{cases} \tag{41}$$

- *change of generators*

  The matrix $A := \left(\begin{smallmatrix} m_1 & n_1 \\ m_2 & n_2 \end{smallmatrix} \right)$ which describes the automorphism σ_b depends on the choice of generators of H. If we change the generators of H from (a_1, a_2) to (a'_1, a'_2) as

$$\begin{cases} a_1 = a'^{\alpha}_1 a'^{\gamma}_2, \\ a_2 = a'^{\beta}_1 a'^{\delta}_2, \end{cases}$$

  then the matrix A changes as[‖]

$$A \to A' = VAV^{-1}, \quad V = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right).$$

  Hence we should regard A and its conjugate VAV^{-1} as equivalent to each other.

In the following we give some examples of the representative systems of the conjugacy classes and the corresponding semidirect product group G.

(i) $p_1 < p_2$

$$A = \left(\begin{array}{cc} m_1 & 0 \\ 0 & n_2 \end{array} \right),$$

  where

$$m_1 = \begin{cases} \pm 1 \\ 2^{e_1 - 1} \pm 1 \quad (e_1 \geq 3, \ p_1 = 2), \end{cases}$$

$$n_2 = \pm 1.$$

The semidirect product group is

$$G = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = b^2 = e, \ b \, a_1 \, b = a_1^{m_1}, \ b \, a_2 \, b = a_2^{n_2} \right\rangle.$$

(ii) $p_1 = p_2 = p \neq 2$

  The set of matrices A falls into four conjugacy classes and their representatives can be chosen as

$$\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \quad -\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \quad \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right), \quad -\left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right).$$

[‖]A similar reasoning which leads to Eq. (39) requires that $p^{e_2 - e_1}$ divides γ.

and the semidirect product groups are

$$G = \langle a_1, a_2, b \mid a_1{}^{N_1} = a_2{}^{N_2} = b^2 = e, \ b\,a_1\,b = a_1{}^{\pm 1}, \ b\,a_2\,b = a_2{}^{\pm 1} \rangle.$$

(iii) $p_1 = p_2 = p = 2$

(a) $N_1 = N_2 = N = 2^e$

- The case $|A| \equiv 1 \pmod{N}$

  We have eight conjugacy classes and a representative system is

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \pm r \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \pm \begin{pmatrix} 1 & 2^{e-1} \\ 0 & 1 \end{pmatrix}, \ \pm \begin{pmatrix} 1 & 2^{e-1} \\ 2^{e-1} & 1 \end{pmatrix}.$$

- The case $|A| \equiv r \pmod{N}$

  We have four conjugacy classes and a representative system is

$$\pm \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}, \ \pm \begin{pmatrix} 1 & 2^{e-1} \\ 2^{e-1} & r \end{pmatrix}.$$

- The case $|A| \equiv -1 \pmod{N}$

  The matrix A is of the form

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

  with $a^2 + bc \equiv 1 \pmod{N}$. It is difficult to carry out complete classification. We only point out that there are at least the following three inequivalent classes;

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sim - \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$r \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sim -r \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- The case $|A| \equiv -r \pmod{N}$

  Some matrices inequivalent to each other are

  $$\pm \begin{pmatrix} 1 & 0 \\ 0 & -r \end{pmatrix}.$$

(b) $N_1 = 2^{e_1}$, $N_2 = 2^{e_2}$ $(e_1 < e_2)$

  There exist matrices A which can not be diagonalized by some regular matrix V. An example of such type of the matrix is

  $$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

  for the cases $(e_1, e_2) = (1, 2)$, $(2, 3)$.

5   A phenomenologically viable example

In this section we consider the effective theory in which the quark/lepton superfields and the Higgs superfields live in $M_4 \times T^2$, where T^2 is given by an elliptic curve E_Λ. It is postulated that $M_4 \times T^2$ is the intersection of two kinds of brane. For instance, we take the brane configuration in which one of the branes is $M_4 \times Y_4$ and the other is $M_4 \times Y_4'$, where Y_4 and Y_4' are different 4-dimensional extra spaces with $Y_4 \cap Y_4' = T^2$. In this paper it is assumed that the extra space is discrete and that the extra space is all of the m-torsion points $E_\Lambda[m]$ of the elliptic curves E_Λ with CM. Our point of view is that the Galois group is nothing but the flavor symmetry for open strings. Thus, we explore the Galois group G relevant to the underlying flavor symmetry including the R-parity. The flavor symmetry yields the selection rule for interactions among quarks and leptons and then governs the stability of proton and the characteristic texture of fermion masses and mixings.

When we take some elliptic curve E_Λ with CM and some number m which represents the size of E_Λ in unit of E_{Λ_0}, the Galois extension field $L = K(E_\Lambda[m])$ induces the abelian Galois group $H = Gal(L/K)$ and also the Galois group $G = Gal(L/\mathbb{Q})$.

The latter is an extension of $\mathbb{Z}_2 = Gal(K/\mathbb{Q})$ by H and is a semidirect product group $\mathbb{Z}_2 \ltimes H$. We now assume that there exists an elliptic curve E_Λ with CM such that the following groups H and G are the Galois groups $Gal(L/K)$ and $Gal(L/\mathbb{Q})$ derived from the Galois extension $L = K(E_\Lambda[m])$:

$$H = \mathbb{Z}_4 \times \mathbb{Z}'_4 \times \mathbb{Z}_N, \tag{42}$$

$$G = \{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_N. \tag{43}$$

Here N is taken as odd. Let us denote the generators of $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}'_4$ and $\mathbb{Z}_N$ by b, a_1, a_2 and a_3, respectively. These generators hold the relations

$$b\, a_i\, b = a_i^{-1} \ \ (i = 1,\ 2), \qquad b\, a_3\, b = a_3 \tag{44}$$

and a_1, a_2 and a_3 are commutable with each other. Furthermore, we suppose that one of two kinds of the D-brane has the degree of freedom of $SU(6)$ gauge group and the other has that of $SU(2)_R$ gauge group. Therefore, we study the $SU(6) \times SU(2)_R$ model with the flavor symmetry designated by the Galois group G.

Here we briefly summarize the parts of the $SU(6) \times SU(2)_R$ string-inspired model which are relevant to our present study. For a more detailed description see Refs. [10].

(i) The gauge group $SU(6) \times SU(2)_R$ can be obtained from E_6 through the $\mathbb{Z}_2$ flux breaking on a multiply-connected manifold. In contrast to the conventional GUT-type models, we have no Higgs fields of adjoint or higher representations. Nevertheless, the symmetry breaking of $SU(6) \times SU(2)_R$ down to the standard model gauge group can take place via the Higgs mechanism.

(ii) It is assumed that the matter content consists of the chiral superfields of three families and the single vector-like multiplet in the form

$$3 \times \mathbf{27}(\Phi_{1,2,3}) + (\mathbf{27}(\Phi_0) + \overline{\mathbf{27}}(\bar{\Phi}))$$

in terms of E_6. The superfields Φ in $\mathbf{27}$ of E_6 are decomposed into two irreducible representations of $SU(6) \times SU(2)_R$ as

$$\Phi(\mathbf{27}) = \begin{cases} \phi(\mathbf{15}, \mathbf{1}) & : & Q, L, g, g^c, S, \\ \psi(\mathbf{6}^*, \mathbf{2}) & : & (U^c, D^c), (N^c, E^c), (H_u, H_d), \end{cases}$$

23

where the pair g and g^c and the pair H_u and H_d represent the colored Higgs and the doublet Higgs superfields, respectively. N^c is the R-handed neutrino superfield and S is an $SO(10)$ singlet. Note that the doublet Higgs and the color-triplet Higgs fields belong to different irreducible representations of $SU(6) \times SU(2)_R$ and so the triplet-doublet splitting problem is solved naturally.

(iii) There are only two types of gauge invariant trilinear combinations

$$
\begin{aligned}
(\phi(\mathbf{15}, \mathbf{1}))^3 &= QQg + Qg^cL + g^cgS, \\
\phi(\mathbf{15}, \mathbf{1})(\psi(\mathbf{6^*}, \mathbf{2}))^2 &= QH_dD^c + QH_uU^c + LH_dE^c \\
&\quad + LH_uN^c + SH_uH_d + gN^cD^c \\
&\quad + gE^cU^c + g^cU^cD^c.
\end{aligned}
$$

We now address ourselves to a discussion of the flavor-charge assignment to each matter superfield. To begin with, we argue the relation between $Gal(K/\mathbb{Q}) = \mathbb{Z}_2$ and the R-parity. The breaking scale of the $SU(6) \times SU(2)_R$ gauge symmetry should be larger than $\mathcal{O}(10^{16}\text{GeV})$ to guarantee the longevity of the proton. Here, it is worth recalling the D-flat condition. When the gauge symmetry is broken at a large scale, the D-flat condition allows the supersymmetry to remain unbroken down to a TeV scale. In order to guarantee the D-flatness with leaving the R-parity unbroken, the effective theory has to contain conjugate pairs of R-parity even matter superfields relative to the gauge group. It is the pair of R-parity even matter superfields that acquires VEV along a D-flat direction. As a consequence of the gauge symmetry breaking at the large scales, most of the R-parity even matter superfields lie at the energy scales much larger than $\mathcal{O}(1\text{TeV})$. By contrast, among R-parity odd matter superfields with three generations the particles of MSSM have to remain massless as low as $\mathcal{O}(1\text{TeV})$. Then, there should be no conjugate pairs of the R-parity odd matter superfields. This means that the R-parity is the quantum number which discriminates between matter superfields with conjugate pair and those without pair. Here we notice that the interchange of the generation matter superfields with the anti-generation ones corresponds to the complex conjugation transformation for Calabi-Yau manifold. On the other hand, in view of the fact that K is a quadratic imaginary field, the automorphism with conjugate properties on the elliptic curves with CM is the subgroup $Gal(K/\mathbb{Q}) = \mathbb{Z}_2$ of the Galois group G. Therefore, we identify $Gal(K/\mathbb{Q}) = \mathbb{Z}_2$ with the R-parity.

Table 5: Flavor-charge assignment to matter superfields.

	Φ_i $(i = 1, 2, 3)$	Φ_0	$\bar{\Phi}$
$\phi(\mathbf{15},\ \mathbf{1})$	$b\,\widetilde{a}_3{}^{q_i}$	$\widetilde{a}_3{}^{q_0}$	$\widetilde{a}_3{}^{\bar{q}}$
$\psi(\mathbf{6}^*,\ \mathbf{2})$	$b\,a_1^2\,\widetilde{a}_3{}^{r_i}$	$a_1^2\,\widetilde{a}_3{}^{r_0}$	$a_1\,\widetilde{a}_3{}^{\bar{r}}$

Next we turn to a discussion of the charge assignment for $Gal(L/K) = H = \mathbb{Z}_4 \times \mathbb{Z}_4' \times \mathbb{Z}_N$. We rewrite H as

$$H \cong \mathbb{Z}_4 \times \mathbb{Z}_{4N} = \langle a_1 \rangle \times \langle \widetilde{a}_3 \rangle \tag{45}$$

and denote the charge of each matter superfield by the notations presented in Table 5. Note that $N = $ odd, so $2N + 1 \equiv -1 \pmod 4$. Consequently, the generator $\widetilde{a}_3$ of $\mathbb{Z}_{4N}$ holds the relation

$$b\,\widetilde{a}_3\,b = \widetilde{a}_3^{2N+1}. \tag{46}$$

Here we assign flavor-charges to matter superfields so as to obtain phenomenologically viable solutions. As in existing phenomenological models, in our approach we cannot definitely settle flavor-charges of matter fields from theoretical arguments. However, we require the mixed-anomaly conditions. These conditions are stringent and the solutions are rather restricted. The flavor-charge of the Grassmann number θ is assigned as $b\,a_1\,\widetilde{a}_3{}^{q_\theta}$. In general, the couplings among matter superfields are given by the nonrenormalizable terms suppressed by powers of $\mathcal{O}(M_S^{-1})$. The explicit forms of the nonrenormalizable terms are determined by the flavor symmetry.

Under the charge assignment given in Table 5, the superpotential in the R-parity even sector can be settled as

$$W_1 = M_S^3 \left[c_0 \left(\frac{\phi_0 \bar{\phi}}{M_1^2} \right)^{2n} + c_1 \left(\frac{\phi_0 \bar{\phi}}{M_1^2} \right)^n \left(\frac{\psi_0 \bar{\psi}}{M_2^2} \right)^4 + c_2 \left(\frac{\psi_0 \bar{\psi}}{M_2^2} \right)^8 \right], \tag{47}$$

where M_S, M_1, $M_2 = \mathcal{O}(10^{19}\text{GeV})$ represent the string scale and $c_i = \mathcal{O}(1)$. Note that $\phi_0\,\bar{\phi}$ and $\psi_0\bar{\psi}$ have both nonzero flavor-charges. As seen from Table 5, the exponent $2n$ (> 0) of the first term on the r.h.s. is determined through the $\mathbb{Z}_{4N}$-invariance. The exponent of the third term on the r.h.s. is constrained both by the $\mathbb{Z}_4$-invariance and by the $\mathbb{Z}_{4N}$-invariance. We choose $2n \sim 4N \gg 8$. Then, we carry

out the minimization of the scalar potential with the soft SUSY breaking mass terms characterized by the scale $\mathcal{O}(1\mathrm{TeV})$. The D-flat solution implies [11]

$$|\langle\phi_0\rangle| = |\langle\bar{\phi}\rangle| > |\langle\psi_0\rangle| = |\langle\bar{\psi}\rangle|. \tag{48}$$

Introducing the notation

$$\xi = \frac{|\langle\phi_0\rangle\langle\bar{\phi}\rangle|}{M_1^2},$$

we have

$$\xi^{2n} = \mathcal{O}(10^{-17}) = \mathcal{O}(\frac{m_W}{M_S}), \qquad \frac{\langle\psi_0\rangle\langle\overline{\psi}\rangle}{M_1^2} = \xi^{\frac{n}{4}+\delta_N}$$

with $\xi^{\delta_N} = \mathcal{O}(1)$. Consequently, the spontaneous breaking of the gauge symmetry occurs in two steps as

$$SU(6) \times SU(2)_\mathrm{R} \xrightarrow{\langle\phi_0\rangle} SU(4)_\mathrm{PS} \times SU(2)_L \times SU(2)_\mathrm{R} \xrightarrow{\langle\psi_0\rangle} G_\mathrm{SM}, \tag{49}$$

where $SU(4)_\mathrm{PS}$ and G_{SM} are the Pati-Salam $SU(4)$ group and the standard model gauge group, respectively. The VEVs turn out to be $|\langle\phi_0\rangle| = \mathcal{O}(10^{18}\mathrm{GeV})$ and $|\langle\psi_0\rangle| = \mathcal{O}(10^{17}\mathrm{GeV})$.

The nonrenormalizable terms in the superpotential induce the low-energy effective interactions through the Froggatt-Nielsen mechanism [12]. The superpotential terms which bring about the effective Yukawa couplings of Φ_i ($i = 0, 1, 2, 3$) take the forms

$$\begin{aligned}
W_Y &= \frac{1}{3!} z_0 \left(\frac{\phi_0\bar{\phi}}{M_1^2}\right)^{\zeta_{00}} (\phi_0)^3 + \frac{1}{2} h_0 \left(\frac{\phi_0\bar{\phi}}{M_1^2}\right)^{\eta_{00}} \phi_0\psi_0\psi_0 \\
&\quad + \frac{1}{2} \sum_{i,j=1}^{3} z_{ij} \left(\frac{\phi_0\bar{\phi}}{M_1^2}\right)^{\zeta_{ij}} \phi_0\phi_i\phi_j + \frac{1}{2} \sum_{i,j=1}^{3} h_{ij} \left(\frac{\phi_0\bar{\phi}}{M_1^2}\right)^{\eta_{ij}} \phi_0\psi_i\psi_j \\
&\quad + \sum_{i,j=1}^{3} m_{ij} \left(\frac{\phi_0\bar{\phi}}{M_1^2}\right)^{\mu_{ij}} \psi_0\phi_i\psi_j. \tag{50}
\end{aligned}$$

The indices i and j run over the generation. Each coefficient in the r.h.s. is supposed to be $\mathcal{O}(1)$. Furthermore, the coefficients of the third, fourth and fifth terms are

assumed to exhibit 3×3 matrices with rank 3. All of the exponents in the above equation are nonnegative integers and determined by the flavor symmetry. Although the parameter ξ is not a very small number, the large hierarchy occurs by raising the ξ to large powers. The colored Higgs mass is given by $z_0 \, \xi^{\zeta_{00}} \langle \phi_0 \rangle$. In order that the colored Higgs gains a large mass around $\mathcal{O}(10^{17} \text{GeV})$, the exponent ζ_{00} should be sufficiently small compared with N. By contrast, the doublet Higgs mass of $\mathcal{O}(10^2 \text{GeV})$ is given by $h_0 \, \xi^{\eta_{00}} \langle \phi_0 \rangle$. Then, the exponent η_{00} should be nearly equal to $4N \sim 2n$. The hierarchical structure of fermion masses are derived via an appropriate flavor-charge assignment for each matter superfield. For instance, the mass matrix for up-type quarks comes from the effective Yukawa terms

$$\mathcal{M}_{ij} \, Q_i \, U_j^c \, H_{u0}, \qquad \mathcal{M}_{ij} = m_{ij} \, \xi^{\mu_{ij}}. \tag{51}$$

In the down-type quark sector D^c-g^c mixing occurs. Similarly, in the lepton sector there appears L-H_d mixing. In both sectors there exist three heavy modes with their masses larger than $\mathcal{O}(10^{10} \text{GeV})$ and three light modes appearing in the low-energy spectrum. In addition, in this model the seesaw mechanism is naturally at work. The Majorana masses of the R-handed neutrinos are induced from the nonrenormalizable term

$$W_M = \frac{f_N}{M_S} \left(\frac{\phi_0 \bar{\phi}}{M_1^2} \right)^{\nu_{ij}} (\psi_i \, \bar{\psi})(\psi_j \, \bar{\psi}) \tag{52}$$

with $f_N = \mathcal{O}(1)$.

In the above superpotential the exponent of each term is determined by the conditions of $\mathbb{Z}_{4N}$-invariance on the F-term

$$
\begin{aligned}
&2n \, d \equiv -2 \, (N+1) \, q_\theta, \\
&8 \, (r_0 + \bar{r}) \equiv 2 \, (N+1) \, q_\theta, \\
&d \, \zeta_{00} \equiv 3q_0 - 2 \, (N+1) \, q_\theta, \\
&d \, \eta_{00} \equiv q_0 + 2r_0 - 2 \, (N+1) \, q_\theta, \\
&d \, \zeta_{ij} \equiv (2N+1) \, q_i + q_j + q_0 - 2 \, (N+1) \, q_\theta, \\
&d \, \eta_{ij} \equiv (2N+1) \, r_i + r_j + q_0 - 2 \, (N+1) \, q_\theta, \\
&d \, \mu_{ij} \equiv (2N+1) \, q_i + r_j + r_0 - 2 \, (N+1) \, q_\theta, \\
&d \, \nu_{ij} \equiv (2N+1) \, r_i + r_j + 2 \, (N+1) \, \bar{r} - 2 \, (N+1) \, q_\theta, \qquad (\text{mod } 4N)
\end{aligned}
\tag{53}
$$

with $d = -(q_0 + \bar{q})$. Furthermore, the additional conditions should be satisfied as

for the mixed anomalies $\mathbb{Z}_M \cdot (SU(6))^2$ and $\mathbb{Z}_M \cdot (SU(2)_R)^2$, where $M = 2$, 4, 4, N corresponding to each subgroup of the Galois group $G = \{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_N$ in order. These conditions are expressed as [13, 14]

$$4\,q_T + 2\,r_T \equiv 18\,q_\theta, \qquad 6\,r_T \equiv 26\,q_\theta \qquad (\mathrm{mod}\ M), \tag{54}$$

where

$$q_T = \sum_{i=0}^{3} q_i + \bar{q}, \qquad r_T = \sum_{i=0}^{3} r_i + \bar{r}.$$

After some manipulation we find a solution with $N = 31$ which satisfies all of the above conditions and reproduces the characteristic texture of fermion masses and mixings. Another solution is found for the case $N = 35$. Here we concentrate on the case $N = 31$. By taking the conventional charge assignment of the Grassmann number $q_\theta = 1$, we obtain the $\mathbb{Z}_{4N}$-charge assignment to each matter superfield as shown in Table 6. Translating $\mathbb{Z}_{4N}$-charges into $\mathbb{Z}'_4 \times \mathbb{Z}_N$-charges, we present $\{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_N$-charges in Table 7. The charge assignment of q_θ offered here implies that all of $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}'_4$ and $\mathbb{Z}_{31}$ are the R-symmetry. In this solution the exponents of the effective interactions are given by $2n = 112$, $(\zeta_{00},\ \eta_{00}) = (2,\ 116)$ and

$$\zeta_{ij} = \begin{pmatrix} 34 & 30 & 22 \\ 30 & 26 & 18 \\ 22 & 18 & 10 \end{pmatrix}_{ij}, \qquad \eta_{ij} = \begin{pmatrix} 38 & 28 & 20 \\ 28 & 18 & 10 \\ 20 & 10 & 2 \end{pmatrix}_{ij},$$

$$\mu_{ij} = \begin{pmatrix} 31 & 21 & 13 \\ 27 & 17 & 9 \\ 19 & 9 & 1 \end{pmatrix}_{ij}, \qquad \nu_{ij} = \eta_{ij} + 30. \tag{55}$$

The ξ-parameter in this solution is related to the well-known λ parameter in the

Table 6: $\mathbb{Z}_{4N}$-charge $\qquad q_\theta = 1$

	$\phi(\mathbf{15},\ \mathbf{1})$	$\psi(\mathbf{6^*},\ \mathbf{2})$
Φ_0	$q_0 = 18$	$r_0 = -19$
$\bar{\Phi}$	$\bar{q} = 49$	$\bar{r} = -4$
Φ_1	$q_1 = 62$	$r_1 = 52$
Φ_2	$q_2 = 82$	$r_2 = 102$
Φ_3	$q_3 = 122$	$r_3 = 18$

CKM matrix as $\xi^4 \simeq \lambda = 0.22$. Taking $\delta_N = 3$, we have the fermion spectra [10]

$$(m_u,\ m_c,\ m_t) \ \simeq\ (\xi^{31},\ \xi^{17},\ \xi) \times v_u, \tag{56}$$

$$(m_d,\ m_s,\ m_b) \ \simeq\ (\xi^{31},\ \xi^{22},\ \xi^{10}) \times v_d, \tag{57}$$

$$(m_e,\ m_\mu,\ m_\tau) \ \simeq\ (\xi^{31},\ \xi^{15},\ \xi^9) \times v_d, \tag{58}$$

$$(m_{\nu_1},\ m_{\nu_2},\ m_{\nu_3}) \ \simeq\ (\xi^8,\ \xi^6,\ 1) \times \frac{v_u^2}{M_S}\xi^{-31}, \tag{59}$$

where v_u and v_d represent the VEVs $\langle H_{u0} \rangle$ and $\langle H_{d0} \rangle$, respectively. The neutrino mass for the third generation m_{ν_3} becomes $\mathcal{O}(10^{-1}\text{eV})$. Thus our model reproduces the orders of magnitude for fermion masses. The CKM matrix is of the form

$$V_{\text{CKM}} \simeq \begin{pmatrix} 1 & \lambda & \lambda^5 \\ \lambda & 1 & \lambda^2 \\ \lambda^3 & \lambda^2 & 1 \end{pmatrix}. \tag{60}$$

Mixing angles in the MNS matrix are

$$\tan\theta_{12}^{\text{MNS}} \simeq \xi, \qquad \tan\theta_{23}^{\text{MNS}} \simeq \xi^3, \qquad \tan\theta_{13}^{\text{MNS}} \simeq \xi^4 \simeq \lambda. \tag{61}$$

This texture of the MNS matrix represents the LMA-MSW solution. All of these results are phenomenologically viable.

Table 7: $\{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_N$-charge $\qquad q_\theta = (-,\ 1,\ 1,\ 1)$

	$\phi(\mathbf{15},\ \mathbf{1})$	$\psi(\mathbf{6}^*,\ \mathbf{2})$
Φ_0	$(+,\ 0,\ 2,\ 18)$	$(+,\ 2,\ 1,\ 12)$
$\bar{\Phi}$	$(+,\ 0,\ 1,\ 18)$	$(+,\ 1,\ 0,\ 27)$
Φ_1	$(-,\ 0,\ 2,\ \ 0)$	$(-,\ 2,\ 2,\ 21)$
Φ_2	$(-,\ 0,\ 2,\ 20)$	$(-,\ 2,\ 2,\ \ 9)$
Φ_3	$(-,\ 0,\ 2,\ 29)$	$(-,\ 2,\ 2,\ 18)$

6 Summary and discussion

In this paper we have explored the underlying flavor symmetry through the arithmetic structure of elliptic curves with CM. It is expected that there are close relations among RCFT, algebraic number theory and elliptic curves E_Λ with CM. We have postulated that the extra space E_Λ, which is given by the intersection of two kinds of brane, is discretized and that the extra space is all of the m-torsion points $E_\Lambda[m]$ ($m \in \mathbb{Z}_+$) of the elliptic curves E_Λ with CM. The endpoints of open strings lie on $E_\Lambda[m]$. $E_\Lambda[m]$ provides the Galois extension field $L = K(E_\Lambda[m])$ which is the extension of field $K(j(E_\Lambda))$ generated by the coordinates of all of $E_\Lambda[m]$. Orientable open strings correspond to an automorphism of L. Hence we are led to the Galois group $G = Gal(L/\mathbb{Q}) = \mathrm{Aut}_\mathbb{Q} L$. Each element of G acts on $E_\Lambda[m]$. Our point of view offered here is that G is the flavor symmetry for open strings and that each element of G corresponds to an orientable open string with free endpoints in the direction along the $E_\Lambda[m]$. We have studied the possible types of the Galois groups. It has been shown that the Galois group G is an extension of $\mathbb{Z}_2$ by some abelian group H and that G is a semidirect product group $\mathbb{Z}_2 \ltimes H$ for the case of the m-torsion points of the elliptic curve. This is an important result of our approach. In general, G is not an abelian group. G possibly contains the dihedral group D_n ($n \geq 3$) but not the symmetric group S_n ($n \geq 4$). We have exhibited a phenomenologically viable example, in which the Galois groups $H = Gal(L/K)$ and $G = Gal(L/\mathbb{Q})$ are taken as $\mathbb{Z}_4 \times \mathbb{Z}'_4 \times \mathbb{Z}_{31}$, and $\{\mathbb{Z}_2 \ltimes (\mathbb{Z}_4 \times \mathbb{Z}'_4)\} \times \mathbb{Z}_{31}$, respectively. In the example it has been shown that the characteristic texture of fermion masses and mixings is reproduced and that the mixed-anomaly conditions are satisfied. In this paper we have assumed

that there exists an elliptic curve E_Λ with CM such that the Galois groups H and G offered here are derived from the m-torsion points of the elliptic curve.

In the above viable example we have chosen $H = \mathbb{Z}_4 \times \mathbb{Z}_4' \times \mathbb{Z}_N$ with $N = 31$. This case is possibly realized if we take $E_\Lambda[m]$ with $m = 311$. Note that $m = 311$ is a prime number, so $N_m = 311^2 - 1$. For the case $N = 35$ we have $m = 41$, in which $N_m = 41^2 - 1$. In both cases the relation $(\#H)|N_m$ is satisfied. The number m represents the size of the extra space E_Λ in unit of E_{Λ_0} which corresponds to the fundamental scale of the string theory. The condition $m \leq \mathcal{O}(10^2)$ ensures that the extra space considered here is sufficiently small.

The Galois group $G = Gal(L/\mathbb{Q})$ is classified according as the homomorphism $\sigma : \mathbb{Z}_2 \to \mathrm{Aut}\, H$ and the factor set f. There are various types of the Galois group which we have not applied to a phenomenological model offered here. From phenomenological point of view, it is favorable for the flavor symmetry to contain the dihedral group D_4. This is due to the fact that the Majorana mass of the third generation is nearly equal to the geometrical average of M_S and M_Z [10]. For the cases of the Galois group containing D_4 we explore the solutions in the same way as the present study. Under some phenomenological requirements we have to solve both conditions coming from the flavor symmetry and mixed-anomaly conditions. To do this, we need to use some ingenious manipulation. Further studies of phenomenologically viable Galois groups on elliptic curves with CM will be reported elsewhere. At present, when we find out the Galois group G relevant to the flavor symmetry, the subsequent problem is open as to how to trace back to the Galois extension field L and the elliptic curves E_Λ with CM. However, our approach proposed here could shed new light on the study of the generation structure of quarks and leptons.

Appendix   General theory of group extension and some examples

In section 4 we have studied the group extension G of $Q = \mathbb{Z}_2$ by an abelian kernel H. In the study we have confined ourselves to the case when the quotient group $G/H \cong \mathbb{Z}_2$ is homomorphically embedded in G. In this Appendix we discuss the general case in which $\mathbb{Z}_2$ is not necessarily embedded as a subgroup in G.

A.1 General theory of the extension $H \lhd G \xrightarrow{\pi} Q$

We sketch the general theory of an extension by an abelian kernel. For more detailed description see Ref. [15]. We first start from the group G. Taking arbitrary section s of the canonical projection $G \xrightarrow{\pi} Q$, we can write $g \in G$ as $g = hs(x)$ with $\pi(g) = x \in Q$, which yields the one-to-one correspondence $G \leftrightarrow Q \times H$ by $g \mapsto (x, h)$. The homomorphic property of π implies that $s(x)s(y)$ and $s(xy)$ are equal up to some element $f(x, y)$ of $\ker \pi = H$, i.e.

$$s(x)s(y) = f(x, y)s(xy). \tag{A.1}$$

The map $f : Q \times Q \to H$ is called the factor set of G associated with the section s. The product defined in G induces a product in the set $Q \times H$ via the section s. In fact, from the equation

$$gg' = hs(x)\, h's(x') = hs(x)h's(x)^{-1}s(x)s(x') = hs(x)h's(x)^{-1}f(x, x')s(xx')$$

and $\pi \circ s = \mathrm{id}_Q$, we obtain the product

$$(x, h)(x', h') = (xx', hs(x)h's(x)^{-1}f(x, x')).$$

In view of the abelian nature of H, the automorphism $\sigma_{s(x)} := s(x)^{-1} \bullet s(x)$ does not depend on s. Hence, dropping s, we can use the abbreviated notation

$$\sigma_x(h') = s(x)\, h'\, s(x)^{-1} =: {}^x h'.$$

Thus the product is rewritten as

$$(x,\, h)(x',\, h') = (x\, x',\ h\, {}^x h'\, f(x, x')). \tag{A.2}$$

The associative law of G leads to the associative law of the above product in $H \times Q$, which requires the cocycle condition

$$f(x, y)\, f(xy, z) = {}^x f(y, z)\, f(x, yz). \tag{A.3}$$

If we change the section s to s'

$$s'(x) = \alpha(x)s(x) \qquad \alpha(x) \in H,$$

f is transformed into

$$f'(x, y) = \alpha(x)\, {}^x\alpha(y)\, \alpha(xy)^{-1} f(x, y). \tag{A.4}$$

32

When this relation holds between f and f', we express as $f' \sim f$.

Reversing all the line of thought, i.e. starting from the set $Q \times H$, we can construct all of the group G which give $G/H \cong Q$. If we introduce a homomorphism $\sigma : Q \to \mathrm{Aut}H, \quad x \mapsto \sigma_x(\bullet) = {}^x(\bullet)$ and a factor set $f : Q \times Q \to H$ which satisfies the cocycle condition (A.3), then we obtain the group G^σ_f whose product is defined by (A.2). Note that if $f' \sim f$, f' and f give the same group, i.e.

$$G^\sigma_{f'} \cong G^\sigma_f \iff f'(x,y) = \delta\alpha(x,y)f(x,y), \quad \delta\alpha(x,y) := \alpha(x)\,{}^x\alpha(y)\,\alpha(xy)^{-1}.$$

The above argument proves the following theorem.

Theorem Let Q be a group, H be an abelian group and σ be a homomorphism $\sigma : Q \to \mathrm{Aut}H, \quad x \mapsto {}^x(\bullet)$, then the set of the group extensions of Q by the kernel H has the one-to-one correspondence with the equivalence class $H^2(Q,H) = Z^2(Q,H)/B^2(Q,H)$, where $Z^2(Q,H)$ and $B^2(Q,H)$ are the two-dimensional cocycle

$$Z^2(Q,H) := \{f : Q \times Q \to H \mid f(x,y)\,f(xy,z) = {}^xf(y,z)\,f(x,yz)\}$$

and the two-dimensional boundary

$$B^2(Q,H) := \{\delta\alpha : Q \times Q \to H \mid \alpha : Q \to H; \delta\alpha(x,y) := \alpha(x)\,{}^x\alpha(y)\,\alpha(xy)^{-1}\},$$

respectively.

Remark. If $f \sim e \in H$, we can choose the section s such that $s(x)s(y) = s(xy)$. Using this homomorphism s, we can regard Q as a subgroup of G. This means that the group G^σ_f is a semidirect product. In section 4 we have studied only this case.

A.2 Extensions of $Q = \mathbb{Z}_2$ by H

Next we proceed to consider the case $Q = \mathbb{Z}_2$. Since $\mathbb{Z}_2$ has only two elements e and x_1, the cocycle condition and the equivalence relation among the factor sets take a simple form. If $s(e) = e \in G$, then Eq. (A.1) leads to $f(x,e) = f(e,y) = e$. Nontrivial values of f are possible only for $f(x_1, x_1)$, which is denoted simply by f. A change of the section $s(x) \to s'(x) = \alpha(x)s(x)$ is allowed only for $\alpha(x_1)$, which is denoted by α. The cocycle condition (A.3) becomes

$$f = \sigma_{x_1}(f) \tag{A.5}$$

and the allowed change of the section induces the change of f as

$$f \to f' = \alpha\,\sigma_{x_1}(\alpha)\,f,$$

which means the equivalence relation

$$f \sim \alpha \, \sigma_{x_1}(\alpha) \, f. \tag{A.6}$$

The product given by Eq. (A.2) leads to the relation among $b := s(x_1)$ and $h \in H$ as

$$b^2 = f, \quad b \, h \, b^{-1} = \sigma_{x_1}(h). \tag{A.7}$$

If $f = e$, i.e. G is a semidirect product, s gives homomorphic embedding $\mathbb{Z}_2 \to G$. We could identify x_1 with $b := s(x_1)$ and, as in Eq. (36), write σ_{x_1} as σ_b. In what follows, we exhibit some examples of the group extension G of $\mathbb{Z}_2$ by an abelian kernel H.

A.2.1 Example.1 $H = \mathbb{Z}_N = \langle a \rangle$

Here we take $N = p^e$ with a prime number p.

- $\sigma_{x_1}(h) = h$

  Any $f = a^k$ $(k \in \mathbb{Z})$ satisfy the cocycle condition (A.5). The equivalence relation (A.6) becomes $f \sim \alpha^2 f \sim \alpha^4 f \sim \cdots$. Thus for odd p all of f's are equivalent to e, which means that the group G is the direct product group $\mathbb{Z}_N \times \mathbb{Z}_2$. For $p = 2$ there are two cases, i.e.

  $$\begin{cases} f = a^k \sim e & (k : \text{even}), \\ f = a^k \sim a & (k : \text{odd}). \end{cases} \tag{A.8}$$

  The former case leads to $\mathbb{Z}_N \times \mathbb{Z}_2$, while the latter leads to

  $$\begin{aligned} G &= \left\langle a, b \mid a^N = b^2 = e, \ bab = a \right\rangle \\ &= \left\langle a' \mid a'^{2N} = e \right\rangle = \mathbb{Z}_{2N}. \end{aligned}$$

- $\sigma_{x_1}(h) = h^{-1}$

  The cocycle condition (A.5) becomes $f = f^{-1}$, whose solutions are $f = e, a^{N/2}$. The latter is possible only for $p = 2$. The group G is a dihedral group

  $$G = \left\langle a, b \mid a^N = b^2 = e, \ bab = a^{-1} \right\rangle,$$

  or a binary dihedral group

  $$G = \left\langle a, b \mid a^N = e, b^2 = a^{N/2}, \ bab = a^{-1} \right\rangle.$$

- $\sigma_{x_1}(h) = h^{\pm r}$

  Similarly to the above consideration, we find

  $$G = \left\langle a, b \mid a^N = b^2 = e, \ bab = a^{\pm r} \right\rangle.$$

A.2.2 Example. 2 $H = \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} = \langle a_1 \rangle \times \langle a_2 \rangle$

We show some examples for $N_1 = p_1^{e_1}$, $N_2 = p_2^{e_2}$.

- $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$, i.e. $\sigma(h_1, h_2) = h_1 h_2^{-1}$
  If $f = e$, we have the semidirect product

  $$G_1 = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = b^2 = e, \ b\,a_1\,b = a_1, \ b\,a_2\,b = a_2^{-1} \right\rangle.$$

  When $p_i = 2$ $(i = 1, \ 2)$, $f = a_i^{N_i}/2$ is allowed. Furthermore, when $p_1 = p_2 = 2$, $f = a_1^{N_1/2} a_2^{N_2/2}$ is also allowed. Correspondingly, we have

  $$G_2 = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = e, \ b^2 = a_2^{N_2/2}, \ b\,a_1\,b = a_1, b\,a_2\,b = a_2^{-1} \right\rangle,$$
  $$G_3 = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = e, \ b^2 = a_1^{N_1/2}, \ b\,a_1\,b = a_1, b\,a_2\,b = a_2^{-1} \right\rangle,$$
  $$G_4 = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = e, \ b^2 = a_1^{N_1/2} a_2^{N_2/2}, \ b\,a_1\,b = a_1, b\,a_2\,b = a_2^{-1} \right\rangle.$$

- $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$, i.e. $\sigma(a_1^{k_1}, a_2^{k_2}) = a_1^{k_2} a_2^{k_1}$

  $$G = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = b^2 = e, \ b\,a_1\,b = a_2, \ b\,a_2\,b = a_1 \right\rangle.$$

- $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix} \right)$, i.e. $\sigma(a_1^{k_1}, a_2^{k_2}) = a_1^{k_1} a_2^{k_1 - k_2}$

  $$G = \left\langle a_1, a_2, b \mid a_1^{N_1} = a_2^{N_2} = b^2 = e, \ b\,a_1\,b = a_1 a_2, \ b\,a_2\,b = a_2^{-1} \right\rangle.$$

References

[1] For example, S. Pakvasa and H. Sugawara, *Phys. Lett.* **B 73** (1978) 61;
   D. B. Kaplan and M. Schmaltz, *Phys. Rev.* **D 49** (1994) 3741 [hep-ph/9311281];
   L. J. Hall and H. Murayama, *Phys. Rev. Lett.* **75** (1995) 3985 [hep-ph/9508296];
   N. Haba, C. Hattori, M. Matsuda and T. Matsuoka, *Prog. Theor. Phys.* **96**

(1996) 1249 [hep-ph/9605238];

C. D. Carone and R. F. Lebed, *Phys. Rev.* **D 60** (1999) 096002 [hep-ph/9905275];

C. Luhn, S. Nasri and P. Ramond, *J. Math. Phys.* **48** (2007) 123519 [arXiv:0709.1447 [hep-th]] and references therein;

E. Ma, *Int. J. Mod. Phys.* **A 23** (2008) 3366 [arXiv:0710.3851 [hep-ph]] and references therein.

[2] D. Gepner, *Phys. Lett.* **B 199** (1987) 380; *Nucl. Phys.* **B 296** (1988) 757.

[3] D. Gepner, *Int. J. Mod. Phys.* **B 22** (2008) 343 [hep-th/0606081]; *Phys. Lett.* **B 654** (2007) 113 [hep-th/0608140].

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986;

J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[5] E. Verlinde, *Nucl. Phys.* **B 300** (1988) 360.

[6] S. Gukov and C. Vafa, *Commun. Math. Phys.* **246** (2004) 181 [hep-th/0203213].

[7] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions*, Springer, Berlin, 1984;

L. Brekke and P. G. O. Freund, *p-Adic numbers in Physics*, *Phys. Rep.* **233** (1993) 1.

[8] S. Lang, *Algebra* revised 3rd Ed., Springer-Verlag, New York, 2002, Chap.VI.

[9] J. J. Rotman, *An Introduction to the Theory of Groups* 4th Ed., Springer-Verlag, New York, 1995, Chap.7.

[10] N. Haba, C. Hattori, M. Matsuda and T. Matsuoka, *Prog. Theor. Phys.* **96** (1996) 1249 [hep-ph/9605238];

N. Haba and T. Matsuoka, *Prog. Theor. Phys.* **99** (1998) 831 [hep-ph/9710418];

T. Matsuoka, *Prog. Theor. Phys.* **100** (1998) 107 [hep-ph/9804329];

M. Matsuda and T. Matsuoka, *Phys. Lett.* **B 487** (2000) 104 [hep-ph/0003239];

M. Matsuda and T. Matsuoka, *Phys. Lett.* **B 499** (2001) 287 [hep-ph/0009077];

Y. Abe, C. Hattori, M. Ito, M. Matsuda, M. Matsunaga and T. Matsuoka, *Prog. Theor. Phys.* **106** (2001) 1275 [hep-ph/0107267].

[11] N. Haba, C. Hattori, M. Matsuda, T. Matsuoka and D. Mochinaga, *Phys. Lett.* **B 337** (1994) 63 [hep-ph/9311298]; *Prog. Theor. Phys.* **92** (1994) 153 [hep-ph/9401332].

[12] C. Froggatt and H. B. Nielsen, *Nucl. Phys.* **B 147** (1979) 277.

[13] L. E. Ibáñez and G. G. Ross, *Phys. Lett.* **B 260** (1991) 291; *Nucl. Phys.* **B 368** (1992) 3;
L. E. Ibáñez, *Nucl. Phys.* **B 398** (1993) 301 [hep-ph/9210211];
K. Kurosawa, N. Maru and T. Yanagida, *Phys. Lett.* **B 512** (2001) 203 [hep-ph/0105136].

[14] Y. Abe, C. Hattori, T. Hayashi, M. Ito, M. Matsuda, M. Matsunaga and T. Matsuoka, *Prog. Theor. Phys.* **108** (2002) 965 [hep-ph/0206232].

[15] J. A. de Azcárraga and J. M. Izquierdo , *Lie groups, Lie algebras, cohomology and some applications in physics*, Cambridge University Press, 1995, Chaps.4 and 5;
K. S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, 1982, Chap.IV.